July 2018

Game over?

Europe's cyber problem

By Camino Mortera-Martinez

CENTRE FOR EUROPEAN REFORM

OPEN SOCIETY
EUROPEAN POLICY
INSTITUTE

Game over?
Europe's cyber problem

By Camino Mortera-Martinez

★ The EU's cyber security plans have been in the spotlight since a series of high profile cyber attacks hit Europe in 2017. But very few people understand what a cyber war really is, how to fight cyber crime and what role, if any, the EU has in all this.

★ Europe's cyber security strategy covers two things: cyber crime, such as online fraud; and cyber attacks, for instance hacking into a nuclear plant. Cyber crime is lucrative, and is expanding rapidly. Cyber attacks have become one of the weapons of choice of governments and criminal organisations around the world. Both cyber threats can come from state and non-state actors.

★ The EU has been good at dealing with cyber crime, by doing what it does best: passing laws. But Europe's ability to prevent and respond to cyber attacks lags behind the offensive cyber capabilities of adversaries like Russia and North Korea.

★ Nobody expects the EU to respond directly to a cyber attack, as only national governments can do this. But Brussels could be doing more to boost Europe's cyber security.

★ There is a gap between the EU's ambitions and its capabilities in cyber security and defence. This gap has resulted in three main problems.

★ First, obtaining digital evidence in cross-border cases is still difficult, both within Europe and outside. This matters because in the borderless world of the internet, vast amounts of European citizens' data sit outside the EU, notably in the US, but also in countries such as China or India.

★ Second, while cyber attacks are on the rise worldwide, the EU is just waking up to the threat and is still deciding what to do about it – and, most importantly, which institutions should be in charge. At the moment, the EU lacks the resources to understand and fight a cyber war.

★ Third, NATO, the EU and the US are still trying to agree on a strategy to respond to cyber attacks, when they can be considered an 'act of war'. There is no agreement on whether or not collective defence should be permissible against non-state actors. Western countries also struggle to agree on ground rules to respond to state-sponsored cyber attacks.

★ There is no simple solution to solve Europe's cyber problems. But there are some modest steps the bloc could take to improve its cyber security.

★ The EU should consider new proposals to facilitate the sharing of electronic evidence both within and outside the EU. The Commission's recent plans to allow member-states to ask companies directly for evidence are unlikely to be agreed in their current shape and do not solve the problem of transatlantic data exchange. The EU could consider replacing current EU-US agreements with a more efficient treaty on digital evidence, and also conclude deals with other countries.

★ The EU should encourage member-states to invest more in cyber security, and co-ordinate their response to major cyber attacks, for example by clearly determining when economic sanctions may be allowed, who should be responsible for implementing them and under which circumstances.

★ Brussels should also step up its efforts to understand the cyber threats it is facing so it can better support member-states in their attempts to counter them. For this, the next European Commission could set up a task force from all the relevant departments of the Commission, to advise it on cyber issues.

★ Finally, Europe and the West should work with technology companies to develop a set of ground rules to define and help attribute cyber attacks.

★ The EU is at a disadvantage because the cyber world's bad actors – unlike the Union – know what they are doing. The challenge for the EU is to learn how to beat these international cyber villains before the next major cyber attack puts Europe's economy and the physical security of its citizens at risk.

Cyber has become the prefix of choice in EU policy-making: everyone wants to talk about the EU's role in relation to cyber security, cyber defence, cyber attacks and cyber crime. Much as counter-terrorism was at the centre of media and public attention in 2015 and migration was in 2016, Europe's cyber security plans have been in the spotlight since a series of high profile cyber attacks in 2017 struck targets including national health systems, banks, and electoral campaigns. And yet very few people understand what a cyber war is, how to fight cyber crime and what role, if any, the EU has in all this.

Cyber threats cross borders, but the EU's efforts to fight them have been meagre to date. Nobody would expect the EU to respond directly to a cyber offensive – after all, the Union is a legal-regulatory organisation rather than a government with a powerful executive function. But there are many other things (from funding to setting standards and co-ordinating national responses) the EU could do to beef up the bloc's cyber security. The 2017 attacks have raised big questions about the European Union's understanding of cyber issues and its ability to deal with security breaches. The increasing incidence of online crime and aggressive cyber tactics from countries like Russia and North Korea mean the EU must up its game.

Europe's cyber security plans cover two different problems: cyber crime (like child pornography or online fraud) and cyber attacks (like disrupting a city's transport network with a virus targeted at its computer systems). Cyber crime and cyber attacks sometimes overlap – like the 'Wannacry' ransomware attack, which blocked computers at large private companies and national service providers including the UK's National Health Service. Both cyber threats can come from both state and non-state actors.[1]

The EU has been good at dealing with more traditional cyber crime, such as identity theft, by doing what it does best: passing laws. But Europe has a more urgent problem to solve: as state-sponsored cyber attacks increase all over the world, there is a gap between the EU's ambitions and its capabilities in cyber security and defence. Europe knows that a cyber war is already happening, but it does not know how to fight it. And crucially, there is no consensus on who should be responsible for responding. Is it NATO, the EU, the national capitals, or a combination of all three?

This policy brief looks at the main cyber threats facing Europe. It assesses the EU's response to them and suggests ways to improve cyber security on the continent.

Cyber threats: A moving target

The cyber world provides criminals, terrorists and ill-intentioned governments with additional tools to fulfil their goals – whether these are stealing money, destabilising a country by attacking critical infrastructure (like nuclear plants), or altering the result of a national election. In fact, it is easier to do some of these things using online tools. It is riskier and more expensive to launch a physical attack on a nuclear plant, for example, than to hack its computer system. And breaking into an electoral campaign to leak compromising information which could influence voters' choices is child's play for experienced hackers.

1: For the sake of brevity, this policy brief will not cover disinformation campaigns, as they do not strictly qualify as cyber attacks, despite being mainly conducted online.

Europe is facing several cyber threats. Each creates a different set of problems and thus requires a different set of solutions. Cyber threats are constantly evolving. But any sustainable cybersecurity strategy should cover, at least, two things: cyber crime and cyber attacks.

Cyber crime
According to the European Commission, the most common types of cyber crime are:

★ Identity theft – when a hacker steals someone's personal information and uses it for financial gain or other purposes;

★ Hacking attacks, which lock users out of computers and information networks, sometimes asking them for money to regain access – also known as 'ransomware attacks';

★ The dissemination of illicit content through online networks (like child pornography).[2]

"Any sustainable cyber security strategy should cover, at least, two things: cyber crime and cyber attacks."

In recent years, there have been some spectacular cases of child pornography and ransomware attacks. In May 2017, the US Federal Bureau of Investigation (FBI) and Europol, the EU's police agency, arrested 870 people in a world-wide investigation of online child sexual abuse. That included the arrest of 368 people in Europe alone, with the operation covering eight EU member-states. The network's ringleader had used the dark web – websites which allow users to conceal their identities – to create a webpage where over 150,000 people accessed and exchanged child pornography. Later that month, hackers allegedly affiliated with the North Korean government launched the WannaCry ransomware attack, which exploited a security weakness in computers using Microsoft operating systems by encrypting data and asking for money to regain access. This attack hit 200,000 computers across 150 different countries.

But there are also less-known (albeit equally dangerous) crimes which can be committed online – or which may be organised online and then carried out in real life. Terrorists regularly use the web to glorify their cause, spot potential recruits and communicate amongst themselves. The so-called Islamic State terrorist organisation (IS) is well known for its IT expertise, and has used the web to launch propaganda and recruitment campaigns (both an essential part of IS's 'online jihad' – which security services refer to, rather inelegantly, as 'Cyberistan'). Cyber stalking, bullying and harassment have also become major problems. According to the Pew Research Centre, four in ten Americans have experienced online harassment.[3] In Europe, a 2014 report showed that 12 per cent of children aged between 9 and 16 years had been cyber bullied.[4]

Cyber crime is costly to society, and it is expanding rapidly. Europol estimates that cyber crime costs the EU some €265 billion per year. In some EU countries, cyber crime now represent half of all crimes.[5] European citizens are increasingly concerned about cyber crime: 87 per cent of them think this kind of crime is important, and the majority of them worry that they will be the victim of a cyber crime one day.[6]

Cyber attacks
Cyber attacks are more difficult to define, as they come in a variety of forms. They range from relatively harmless actions (like replacing a government website with an adversary's material) to economically significant attacks (hacking systems so banks and stock markets could not operate) and life-threating strikes (such as meddling with air traffic control).

In 2007, the Estonian government decided to move a bronze statue of a Red Army soldier (which commemorates the Soviet victory over Nazism) from the centre of Tallinn to the outskirts. This sparked outrage amongst some members of the Russian-speaking minority in Estonia, who took to the streets. One person died and over 150 were injured in the riots that ensued. Two days later, the country was hit by a series of cyber attacks. Hackers launched a string of 'denial of service' attacks, which flooded the IT systems of banks, news outlets and government organisations with requests to the extent that their servers went down. For days, Estonians could not access cash machines or online banking services; government officials could not send or receive emails; and newspapers and broadcasters could not deliver the news.[7] When a panicked Estonian government turned to the EU for help, it hit a wall: it was the first time the Council of Ministers had heard of a massive cyber attack against a member-state and the EU simply had no strategy (or resources) in place to help. To this day, even after confirming that the IP addresses used to launch the attack were in Russia, neither the Estonian government nor the EU have been able to prove that the Russian authorities were behind Europe's first major cyber incident.

Russia was also allegedly responsible for a more recent attack which temporarily shut down Ukrainian banks

2: European Commission, 'Special Eurobarometer 464a: Europeans' attitudes towards cyber security', Brussels, September 2017.
3: Monica Anderson, 'Key trends shaping technology in 2017', Pew Research Centre, December 2017.
4: European Parliament, 'Cyberbullying among young people', July 2016.
5: European Council: 'EU cybersecurity', 2017.
6: European Commission, 'Europeans' attitudes towards cybersecurity', special Eurobarometer, September 2017.
7: Damien McGuinness, 'How a cyber attack transformed Estonia', BBC news, April 27th, 2017.

and power facilities, and affected Kyiv's airport and metro system. The attack, dubbed NotPetya because of its similarity with a previously known ransomware called Petya, spread to countries in Europe and beyond, including Britain, France, Poland and the US. Like WannaCry, NotPetya also locked users out of computers and demanded a ransom. But unlike it, those affected by NotPetya could not pay to get their data back because the attackers eventually shut down the email address provided to confirm payment, without explanation. NotPetya hit 2,000 users around the world and is estimated to have cost companies more than $1.2 billion in total.

Western governments have also occasionally used cyber weapons. In 2009 and 2010, the US and Israeli governments allegedly developed a virus to hack Iranian uranium-enrichment nuclear plants.[8] The so-called Stuxnet cyber attack was probably the most successful strike anywhere, as it resulted in around 1,000 of Iran's 5,000 nuclear centrifuges tearing themselves apart, setting its nuclear programme back significantly.[9]

"Like traditional warfare, cyber attacks can be used to retaliate against aggressions in the real world."

But cyber attacks are not only state-sponsored. Private individuals and non-state actors, like terrorist groups, also use hacking tools to disrupt networks. IS even has a division especially devoted to hacking, called the United Cyber Caliphate. Although IS cyber terrorists are better at hiding information (using encryption) and publicising themselves (using social media), they have still managed to launch some successful, minor attacks against Western governments – in 2015, the IS hacking division published a 'kill list' of 1,400 US military and government personnel that it had stolen from the US government.

Much like traditional warfare, cyber attacks can also be used to retaliate against aggressions in the real world: after the poisoning of former Russian double agent Sergei Skripal and his daughter in the UK, allegedly by individuals linked to the Russian government, the British government hinted at the possibility of launching a cyber attack against Russia in retaliation.[10] The idea was later dropped, but it showed that a cyber war is no longer confined to science-fiction novels. The cyber world offers ways to retaliate against unlawful state acts that go further than sanctions but fall short of physical force, widening the field of conflict.

Cyber attacks and cyber crime sometimes overlap: the WannaCry ransomware attack hit private computers, but also the UK's National Health Service (NHS). The attack disrupted computers at one-third of NHS hospital groups in England, including 595 doctors' practices. Thousands of appointments and operations had to be cancelled, with patients having to travel further to access emergency services.[11] A day before Emmanuel Macron was elected as France's president, on May 7th 2017, hundreds of his campaign documents were leaked online, in an effort to influence the election. The French electoral commission, a watchdog, warned that anyone re-publishing the information would face jail time, as disseminating private documents contravenes French law.

Does Europe speak cyber? The EU's cyber security plans

The European Union has proved better at dealing with cyber crime than with state-sponsored cyber attacks. This makes sense: the EU is a legal organisation, which is much more skilled at regulating things than it is at responding to crises, because it does not have the executive powers to do so.

The EU has been working on harmonising rules on cyber crime since 2001, when the bloc launched its first law on online fraud.[12] A 2013 directive aligned national laws and penalties for cyber crime.[13] The directive required all member-states to criminalise attacks against information systems, for example illegally accessing or disrupting an online banking network, or stealing someone's identity online. It mandated that cyber crime should carry penalties of imprisonment of up to five years, but member-states could increase them if the crime was committed under 'aggravating' circumstances, such as pretending to be somebody else. The directive also created a new EU-wide category of crime: producing, selling or distributing tools, like malicious software ('malware') to commit cyber crime. Finally, it boosted judicial and police co-operation by setting up rules to determine which country is responsible for prosecuting cross-border cyber crime and asking member-states to prioritise urgent cases through the use of an EU-wide round-the-clock network of 'contact points'. Each member-state should appoint a 'contact point', who should be available to provide relevant information and legal and technical support for cross-border investigations at any time. The directive has been written into national law by all member-states except for

8: Ellen Nakashima and Joby Warrick, 'Stuxnet was work of U.S. and Israeli experts, officials say', *The Washington Post*, June 2nd 2012.
9: David E. Sanger, 'Obama order sped up wave of cyber attacks against Iran', The *Ne*
10: Tom Parfit poisoning', acks May over Russian spy , March 13th 2018.
11: National Audit Office, 'Investigation: WannaCry cyber attack and the NHS', October 2017.
12: In March, the Council of Ministers approved a new law to update EU rules against online fraud. The European Parliament is due to approve it later this year.
13: Directive 2013/40/EU on attacks against information systems.

Denmark, which opted out. The EU has also reviewed its counterterrorism laws to criminalise terrorist offences carried out online.[14]

Europol, the EU's police agency, set up its Cybercrime Centre (EC3) in 2013. It is a central hub for sharing intelligence on cyber crime, and supports member-states' operations and investigations. EC3 also identifies new threats and developments in cyber crime and has a team of forensic experts who analyse files in search of malware. In 2016, Europol's cyber team supported the investigation, and subsequent dismantling, of the online criminal network 'Avalanche', which attacked online banking systems worldwide. Europol was also involved in an operation against airline ticket fraud, where 193 people were arrested for offering fake plane tickets.

"There is a limit to what the EU can do in the area of cyber security."

Compared to cyber crime, which it started tackling almost 20 years ago, cyber attacks are a relatively recent area of concern for the EU. The European Commission launched its first cyber security strategy in 2013, five years after Russia's alleged cyber attack against Estonia. At that time, 11 out of 28 member-states did not have computer emergency response teams in place. A similar number of countries did not even have a national cyber strategy. So the EU faced a gap between its legislative ambition and the actual capabilities of its member-states. Subsequent initiatives have tried to bridge that gap, but differences still exist. In 2015, at a high time of cyber attacks (300 million records were leaked from public and private organisations during that year), the EU unveiled its Digital Market Strategy.[15] The strategy acknowledged the need to involve the private sector in its efforts through a partnership with the industry association, the European Cyber Security Organisation (ECSO). Despite this initiative, the strategy failed to address one of the industry's main concerns: who is ultimately responsible for issuing the rules the private sector needs to follow – the EU or the member-states?

The Commission presented its most recent cyber security package in September 2017. The plan includes some sensible initiatives. But these are mainly long-term and unlikely to deliver immediate results – something which can be problematic in a rapidly evolving policy environment like the cyber domain. The strategy includes, for example, a blue-print for co-ordination between member-states in the case of major incidents. More importantly, it introduces an EU-wide certification scheme for technology products – so all ICT goods and services manufactured and provided in the EU will meet the same security standards. At the moment, cyber security requirements are different across the EU. This not only makes it more difficult for companies to trade across borders, but it also means that consumers are more protected against cyber crime in some countries than others (for example, some European banks offer the option of confirming financial transactions by SMS when they identify suspicious activity in a client's bank account). But cyber-certification is not a silver bullet. It is, for example, very difficult to certify that a cloud service complies with EU standards at all times. Cloud services, like Apple's system to store pictures, or Salesforce, a database of corporate contacts, are made up of thousands of software bits which update several times per day, so that the information stored is kept up to date. A cyber certificate issued on Tuesday 10 am may not be valid two hours later – although the EU has been working on bringing together different cyber security certification schemes, specifically designed for cloud services.[16]

The EU's 2017 cyber security package also suggested strengthening the mandate of the EU cyber agency ENISA, by making it a permanent agency and doubling its budget to €23 million. ENISA will be tasked with helping member-states, EU institutions and businesses in the event of a cyber attack, as well as with improving intelligence-sharing. Established in 2004, ENISA has a team of around 60 people and is based in Heraklion, on the Greek island of Crete.

In July 2016, the EU adopted a directive on the security of network and information systems.[17] It requires member-states to be properly equipped to protect themselves against cyber attacks, for example by setting up specialised teams and ensuring that businesses providing essential services have taken the appropriate security measures.

The EU's efforts to protect Europe from cyber crime and cyber attacks are promising. But the cyber world is complex, and moves fast. Legal obstacles and member-states' different capabilities and attitudes towards cyber security mean that there is a limit to what the EU can do in this area.

14: Directive (EU) 2017/541 on combating terrorism.
15: Paul Szoldra, 'The 9 worst cyber attacks of 2015', *Business Insider*, December 29th 2015.
16: European Union Agency for Network and Information Security (ENISA): Cloud computing certification – CCSL and CCSM.
17: Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union.

Europe's cyber problem…

The gap between the EU's capabilities and its ambitions on cyber has resulted in three main problems.

First, while the bloc has done well in tackling cyber crime, obtaining digital evidence in cross-border cases is still difficult. Crime (cyber and otherwise) often leaves digital footprints (a Whatsapp conversation or internet searches, for example). These traces can be used as evidence in criminal investigations. But, because the cyber world does not have borders, often police and judges conducting an investigation in a member-state have to ask another member-state or even a third country for the evidence. This is relatively straightforward within the EU: member-states rely on the EU principle of mutual recognition of judicial decisions to issue direct requests to internet companies. For example, a French judge prosecuting a terrorist could ask the Irish branch of Facebook to give them access to anything the suspect had posted or shared. Judicial authorities can also ask their counterparts in other member-states to handle e-evidence directly, through, for example, the European Investigation Order – an EU law requiring member-states to carry out investigative measures on behalf of another country within a deadline of three months. But it is much more complicated when the e-evidence sits in a third country, like the United States.

"There is a gap between the EU's capabilities and its ambitions on cyber security."

Currently, EU countries rely on Mutual Legal Assistance treaties (MLATs) to request evidence from America and other international partners, like Japan. MLA requests take an average of ten months and in those cases where evidence is finally handed over, it is often too late and/or out-of-date for the prosecution. That is why EU countries prefer to use other channels: US tech companies like Facebook or Microsoft receive an average of 100,000 direct data requests per year from EU governments. (EU member-states issue an average of 4,000 official data requests through the EU-US MLA agreement). Currently, there is no law governing direct requests to companies so the whole system works on the assumption that tech firms will simply hand over information to law enforcement authorities. Such requests put firms in a difficult position, because they are also required to comply with EU data protection rules. This situation compromises both Europe's security and the privacy of its citizens.

This legal gap has already caused problems on both sides of the Atlantic. The US government is suing Microsoft, which has refused to provide evidence stored on a server located in Ireland. The EU is looking at ways to work around similar problems. The Commission presented a proposal on obtaining cross-border evidence on April 17th. The Commission's proposal would allow national authorities to circumvent MLATs by issuing direct requests to companies. Under the EU's new plans for a 'European Production Order', private companies will have a deadline of ten days (or six hours in urgent cases) to provide electronic evidence like emails to courts. Companies will have to submit data even if they are not located in the EU.[18] This proposal is unlikely to be approved by the European Parliament, as it raises serious privacy concerns. It will also be met with strong resistance from the US: because of stringent EU data protection laws rolled out in May 2018, EU companies will not be allowed to respond to direct requests coming from America unless there are specific bilateral deals between EU countries and the US. But the Commission's proposal would force American companies to comply with requests coming from Europe.[19]

Second, as cyber attacks have become one of the weapons of choice of states around the world, the EU is lagging behind its antagonists, especially Russia and North Korea. This is because the EU is just waking up to cyber threats and is still deciding what to do about them – and, most importantly, which institutions should be in charge. The EU does not have competence on matters of national security, which is still in the hands of the member-states. Similarly, competences over military capabilities are largely in the hands of national capitals, with some powers at the NATO and EU level.[20] But cyber security is a cross-border issue where the EU can certainly add value.

At the moment, the EU lacks the resources to understand, and fight a cyber war. Those resources are confined to a few member-states. Estonia is now world-leading both on e-government and on the cyber security and defence measures needed to make it work, with several government agencies involved in protecting the country's advanced 'e-administration', and a budget of €4 million devoted to cyber security. France is planning to double the number of 'digital soldiers' within its army to 2,600 and hire 600 civilian experts on cyber by 2019, and Britain set up a National Cyber Security Centre in 2016. While the EU tries to agree on a common answer to the thorny question of what to do when a country launches a cyber attack against European interests, Europe's security – and

18: A new 'European Preservation Order' would allow courts to ask companies not to delete certain pieces of information, as they may become relevant in an investigation later on.

19: Catherine Stupp, 'Leaked EU overhaul gives tech companies 10 days to share 'e-evidence' data with police', *Euractiv*, March 30th 2018.

20: For example, the European Defence Agency, an EU body, delivers trainings on cyber defence planning and decision making for member-states' military headquarters; NATO has a "Rapid Reaction Team" available to help its member countries at any time in case of a cyber attack.

its economy – are in danger. Brussels has limited powers to counter state-sponsored cyber attacks. This does not help member-states – under-resourced EU countries may find themselves relying on a European Union that is unable to help, as was the case for Estonia in 2007. It is also not good for European companies. The lack of clarity over who should do what in the event of a cyber attack is confusing also for the private sector, which does not know who to turn to for help, or which rules to follow.

"The West is still trying to agree on a strategy to respond to state-sponsored cyber attack."

The third problem goes beyond European borders. NATO, the EU and the US are still trying to agree on a strategy to respond to cyber attacks when they can be considered an 'act of war'. There is no agreement on whether or not collective defence should be permissible against non-state actors, partly because attributing a cyber attack to a particular organisation is generally difficult. Western countries also struggle to agree on ground rules to respond to state-sponsored cyber attacks. First, unlike in traditional warfare, attributing a cyber attack to a specific country is not easy. Even in cases where intelligence agencies have proof of a country's malicious activity, blaming a single actor is difficult. Britain and the US blamed North Korea for the 2017 WannaCry attack. But the attack exploited a vulnerability in the Microsoft Windows operating system, first discovered by the US National Security Agency (NSA). The lapse was leaked and posted online by a group of hackers known as the 'Shadow Brokers' shortly before the attack, making it available for anyone with the resources to use it. In cases like this, who is to blame? The NSA, for not protecting its dangerous discovery? The hackers, for enabling the attack? Or the actual perpetrator (thought to be North Korea's Lazarus hacking group)?

Second, while state-sponsored cyber attacks can cause damage akin (at least in terms of financial cost) to traditional acts of war, they hardly ever follow the same pattern. For example, a Russian cyber attack against a Bulgarian nuclear plant may be rather straightforward (a foreign attack against a country's critical infrastructure) and could trigger economic sanctions and other means of retaliation. But modern cyber attacks are rarely that simple. Ransomware strikes like WannaCry, targeting both national infrastructure and private interests, are much more difficult to fight, as a response needs to involve both the state and the private sector. Companies like Microsoft or Facebook are increasingly the target of cyber attacks which also compromise national security interests. And yet, there are no international rules setting out what a company can, or cannot do when such attacks happen. Cyber fighters know this and are increasingly targeting state interests by attacking the private companies that provide on-line services to governments.

…and how to solve it

The cyber world is relatively new and complex. No country in the world is immune to cyber attacks and cyber crime. There is no simple solution to solve Europe's cyber problems. But there are some modest steps the EU could take to improve its cyber security.

First, the EU should consider new proposals to facilitate the sharing of electronic evidence both within and outside the EU. The proposed EU Production Order is a good first step to handle e-evidence in Europe but is unlikely to be agreed in its current shape and will not facilitate transatlantic co-operation – rather the contrary. It will also have the additional problem of outsourcing significant law enforcement powers to private companies. Problems of jurisdiction also complicate international co-operation. This matters because in the borderless world of the internet, vast amounts of European citizens' data sit outside the EU, notably in the US, but also in countries such as China or India – where many large companies have outsourced their IT services. The current international treaty governing access to evidence between the EU and the US (the EU-US MLAT) does not work because the EU's stringent privacy standards and the US' rigorous procedural requirements for handling evidence make it too slow and inefficient. The EU and the US have been discussing a reform to this treaty for a long time. But Europe needs a clearer legal framework to handle requests for evidence stored outside the EU. For example, the EU and the US could consider a dedicated treaty to govern access to digital evidence. Such a treaty should address not only government-to-government requests but also government-to-company ones – while fully respecting the privacy of European citizens and international rules on co-operation on criminal matters.

If governments can get digital evidence more quickly and efficiently through official channels, law enforcement and judicial authorities will be able to obtain the information they need without banning encryption and other privacy-protecting technologies. At present, state authorities often require software companies to leave a 'back door' open for law enforcement – a practice which also leaves secure data vulnerable to penetration by criminals or hostile state actors; banning encryption altogether would be another step to make life easier for law enforcement, but at the cost of putting private individuals and firms at more risk. Better and easier to use official channels would also help to ensure that security agencies do not

overreach their competences. This could, in turn, reduce the cases where sweeping powers have led to breaches of fundamental rights other than privacy.

Additionally, the EU could also explore ways to improve co-operation with other partners. This may not always be easy: while collaborating with foreign authorities in law enforcement operations against cyber crime, European governments may need to reveal vulnerabilities in their own systems which could be used against them later. But this should not discourage the EU from strengthening its ties with both developed and emerging economies affected by cyber crime and able to help in the fight against it. A good place to start would be a set of mutual legal assistance treaties between the EU, India and China. Because they would be written from scratch, these MLATs could address the problem of e-evidence by inserting specific clauses on it.

"The EU should make sure that there is a consistent approach to cyber security across Europe."

Second, the EU should focus on acquiring the knowledge and resources to build a robust cyber security strategy. At the moment, the EU lacks the competence and operational capacity to respond to state-sponsored cyber attacks. But the cyber threat is a transnational challenge, and the EU can do two things to help tackle it

First, it can make sure that there is a consistent approach to cyber security across Europe. The EU should encourage member-states to invest in new, up-to-date technology and trained personnel, and make sure they are ready to respond to cyber attacks, for example by funding projects on cyber defence capabilities through the European Defence Fund.[21] ENISA could also help with that. Second, it can co-ordinate member-states' responses to countries which either conduct cyber campaigns or allow them to be launched from their territory. The EU has successfully co-ordinated economic sanctions in recent years in response to threats such as the Iranian nuclear programme or Russia's invasion of Ukraine. In 2017, the EU came up with a cyber diplomacy toolbox to streamline Europe's response to cyber attacks.[22] The toolbox includes measures ranging from political declarations to economic sanctions. But this toolbox has yet to be transposed into effective actions and policy instruments.[23] The EU should begin by clearly defining which elements are part of this toolbox, who can use them and when.

To play a successful role in supporting member-states' responses against cyber attacks, the EU must begin by having a clear definition of the forms of cyber activity, and what impact it has on all its policies – from trade, to crime, to the rule of law. Hackers have begun to exploit companies' weaknesses for the purpose of insider trading; cross-border networks of smugglers – of people and of illicit goods – use social media and the dark web to carry out their activities in Europe; and election hacking and meddling threaten European democracies and the rule of law. A good place to start understanding the impact of cyber in Europe would be for the next European Commission to set up a task force from all the relevant Commission departments and EU agencies to advise on cyber issues. This task force would help the European Commission in making sure it is up-to-date and ready when the next cyber attack happens. The Commission has an important role to play because, unlike other international institutions, such as NATO, it can reach out both to the private sector and to civil society and human rights organisations. The Council of Ministers already has a similar group – the High Level Working Group on Cyber, chaired by a representative of the country holding the Council's rotating presidency. ENISA is supposed to support member-states, but is currently too under-resourced and isolated, both institutionally and geographically, to play that role adequately.

Finally, both Brussels and national capitals should join the conversation about the need for clearer international rules governing cyber attacks. NATO and the UN have said that international law (including the 1949 Geneva Conventions, which govern the way warfare is conducted) apply to cyber space.[24] Because the Geneva Conventions and their additional protocols only apply during conflicts, they are not a suitable basis for governing cyber attacks in peace time: such attacks can happen at any time and come from a variety of actors. So the private sector is calling for new rules which would apply, exclusively, to the cyber world. Microsoft has asked governments around the world to sign what they call a Digital Geneva Convention.[25] Such a convention would have three pillars:

21: President Juncker has encouraged member-states to use the framework of Permanent Structured Co-operation (PESCO) and the European Defence Fund to support projects on cyber defence. European Commission, 'State of the Union 2017 - Cybersecurity: Commission scales up EU's response to cyber-attacks', Brussels, September 2017.

22: Council of Ministers, 'Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox")', Brussels, June 7th 2017.

23: Erica Moret and Patryk Pawlak, 'The EU Cyber Diplomacy Toolbox: towards a cyber sanctions regime?', European Union Institute for Security Studies brief, July 2017.

24: United Nations, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, June 24th 2013. NATO Wales Summit, September 4th and 5th 2014. The Geneva Conventions are part of international war rules, or jus in bello. The definition of jus in bello is taken from the International Committee of the Red Cross.

25: Brad Smith, Keynote address at the RSA 2017, 'The need for a Digital Geneva Convention', San Francisco, February 14th 2017.

first, signatory states should refrain from launching cyber attacks; second, the private sector should sign a 'Tech Accord' which would lay down guidelines to protect its customers from cyber attacks; third, the parties to the Convention would set up an independent agency which would investigate and attribute responsibility for cyber attacks. But a wide-ranging cyber treaty is unlikely to happen anytime soon: because of disagreements between its member-states on what should be considered a cyber attack and how to fight it, the UN has been unable to elaborate on the simple principle that international law applies to cyber space. Even if countries overcame their differences on cyber issues, it is unclear what technical mechanism they would use to verify compliance.[26] And a Digital Geneva Convention would not solve the problem of cyber attacks by non-state actors – unless somebody managed to convince international terrorist organisations and hacking groups to sign an international treaty.

As NATO Deputy Secretary General Rose Gottemoeller says, cyber security may be a relatively new area of concern for nation-states, but cyber space does not have to be the 'wild wild web'.[27] Current international rules, including customary or unwritten rules, apply to cyber warfare. But these rules are not enough, as they fail to address important questions such as what the role of the private sector should be, and how to work around problems of attribution. Microsoft's Digital Geneva Convention may be too ambitious for now, but it does contain some elements worth considering. An international Tech Accord would help to clarify the position of private companies while reassuring consumers. Establishing a neutral, non-governmental agency which could assign responsibility for cyber attacks may be far-fetched at present, but eventually, countries in Europe and elsewhere will need to agree on a set of principles to solve the problem of attribution. If the West managed to agree even on a basic set of rules, others, like China, might eventually be incentivised to follow.

Conclusion

There is no cure-all for Europe's cyber headaches. Access to cross-border digital evidence is still difficult in a world where online crimes are on the rise; the EU has not yet grasped the full impact of state sponsored cyber attacks; and the West has failed to agree on international rules to attribute, and respond, to attacks damaging private and national security interests.

The EU's ambitions on cyber do not match reality: the bloc does not have either the operational or the legal capacity to prosecute cyber criminals or retaliate against a major cyber attack. But Brussels could be doing more to boost Europe's cyber security. The EU could further improve rules governing access to digital evidence, both within and outside the Union, for example by seeking a transatlantic treaty. Brussels should also step up its efforts to understand the cyber threats it is facing so it can better support member-states in their attempts to counter them. For this, the next European Commission could set up a task force to advise it on cyber issues. The EU should also encourage member-states to invest more in cyber security, and co-ordinate their response to major cyber attacks, for example by implementing the EU's cyber diplomacy toolbox. Finally, Europe and the West should work with technology companies to develop a set of ground rules to define and attribute cyber attacks.

The EU should start by recognising that it is now at a disadvantage because the cyber world's bad actors – unlike the Union – know what they are doing. The challenge for the EU is to learn how to beat these international cyber villains. Otherwise, a major cyber attack could endanger not only the EU's economy but the physical security of its citizens.

Camino Mortera-Martinez
Senior research fellow, Centre for European Reform

July 2018

This publication is supported by the Open Society European Policy Institute.

OPEN SOCIETY
EUROPEAN POLICY
INSTITUTE

26: Tomáš Minárik and LTC Kris van der Meij, 'Geneva Conventions apply to cyberspace: No need for a Digital Geneva Convention', NATO Co-operative Cyber Defence Centre of Excellence, July 18th 2017.

27: Rose Gottemoeller speaking at an event in Brussels in February 2018.